New Family of Binary Sequences with Low Correlation and Large Size

Nam Yul Yu and Guang Gong, *Member, IEEE*

Abstract

For odd $n = 2l+1$ and an integer $\rho, 1 \leq \rho \leq l$, a new family $\mathcal{S}_o(\rho)$ of binary sequences with period $2^n - 1$ is constructed. For a given ρ, $\mathcal{S}_o(\rho)$ has maximum correlation $1 + 2^{\frac{n+2\rho-1}{2}}$, family size $2^{n\rho}$, and maximum linear span $\frac{n(n+1)}{2}$. Similarly, a new family of $\mathcal{S}_e(\rho)$ of binary sequences with period $2^n - 1$ is also presented for even $n = 2l$ and an integer $\rho, 1 \leq \rho < l$, where maximum correlation, family size, and maximum linear span are $1 + 2^{\frac{n}{2}+\rho}$, $2^{n\rho}$, $\frac{n(n+1)}{2}$, respectively. The new family $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$) contains Boztas and Kumar's construction [1] (or Udaya's [2]) as a subset if m-sequences are excluded from both constructions. As a good candidate with both low correlation and large family size, the family $\mathcal{S}_o(2)$ is discussed in detail by analyzing its distribution of correlation values.

Index Terms

Family of binary sequences, sequences with low correlation, linear span.

I. Introduction

In code division multiple access (CDMA) communication systems, pseudo-noise *sequences* are assigned to distinct users in a common channel at the same time [3]. To distinguish each user and minimize interference due to others, we must have low *cross correlation* between distinct sequences. Furthermore, we must also have low *autocorrelation* between a sequence and its time shift version in order to acquire the accurate phase information at the receiver. The capacity of the CDMA system can be increased by assigning a large number of such sequences to distinct users. Consequently, a family of sequences with low correlation and large family size plays important roles in CDMA communication systems.

The construction of a family of binary sequences is based on the combination of a binary m-sequence and its decimations such that the resulting sequences have low correlation achieving the well known lower bounds derived by Welch [4] and Sidelnikov [5]. For odd n, Gold sequences [6] constitute one of the family with optimal low correlation achieving the Sidelnikov bound. A family of Kasami sequences [7] gives sequences with optimal low correlation achieving the Welch's lower bound for even n. In order to obtain binary sequences with large linear span as well as low correlation, Boztas and Kumar constructed a new family of binary sequences for odd n, so called *Gold-like sequences* [1]. It has the same period, family size, and maximum correlation with the family of Gold sequences, but larger linear span giving better potential cryptographic properties. Similarly, Udaya constructed a new family of binary sequences with low correlation similar to Kasami sequences but larger linear span for even n [2]. Kim and No generalized these two constructions [8]. However, it resulted in the decrease of maximum linear span and the increase of maximum correlation. In [9], Chang *et al.* showed that a binary cyclic code based on three-term sequences [10] has five-valued nonzero weight distribution, which is identical to a dual code of a triple error correcting BCH code. From these cyclic codes, equivalent families of binary sequences with six-valued correlation of maximum $1+2^{\frac{n+3}{2}}$, family size 2^{2n}, and maximum linear span $3n$, can be constructed. These are all known cases of binary signal sets having linear span greater than $2n$ and good correlation.

In this paper, a new family $\mathcal{S}_o(\rho)$ of binary sequences with period 2^n-1 is constructed for odd $n=2l+1$ and an integer $\rho, 1 \leq \rho \leq l$. For a given ρ, maximum correlation of sequences in $\mathcal{S}_o(\rho)$ is $1+2^{\frac{n+2\rho-1}{2}}$ and its family size is $2^{n\rho}$. Similarly, a new family $\mathcal{S}_e(\rho)$ of binary sequences with period 2^n-1 is also presented for even $n=2l$ and an integer $\rho, 1 \leq \rho < l$, where maximum correlation and family size are $1+2^{\frac{n}{2}+\rho}$ and $2^{n\rho}$, respectively. The maximum and minimum linear span of sequences in both $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$ are $\frac{n(n+1)}{2}$ and $\frac{n(n-2\rho+1)}{2}$, respectively. As ρ increases, we can obtain a new family $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$) of exponentially increased family size with linear increase of maximum correlation from its optimal value. Since the family $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$) contains $\mathcal{S}_o(\rho-1)$ (or $\mathcal{S}_e(\rho-1)$) as a subset, it contains $\mathcal{S}_o(1)$ (or $\mathcal{S}_e(1)$) as a subset. Here, $\mathcal{S}_o(1)$ is the family of Gold-like sequences constructed by Boztas and Kumar, and $\mathcal{S}_e(1)$ is the one constructed by Udaya, where m-sequences are excluded in both constructions.

For a specific application, we can choose a proper value ρ and corresponding family $\mathcal{S}_o(\rho)$ or $\mathcal{S}_e(\rho)$. For example, a small value of ρ can be chosen if low correlation is more crucial than large family size in the application. Otherwise, we can choose a large value of ρ in order to get large family size. The family $\mathcal{S}_o(2)$ with maximum correlation $1+2^{\frac{n+3}{2}}$ and family size 2^{2n} is an example for good compromise between correlation and family size.

This paper is organized as follows. In Section II, we give some preliminaries on concepts and definitions of codes and sequences. Also, we review the weight distribution of a linear cyclic subcode of the second order *Reed-Muller* code [11], which will be used to investigate the distribution of correlation values of sequences in our new family. In Section III, we present new families $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$ of binary sequences with period 2^n-1 for odd and even n, respectively, and analyze the correlation and linear span of each family. In Section IV, the distribution of correlation values of the sequences in $\mathcal{S}_o(2)$ is derived in terms of the weight distribution of a linear cyclic subcode of the second order Reed-Muller code. Concluding remarks are given in Section V.

II. Preliminaries

The following notations will be used throughout this paper.

- $\mathbb{F}_Q = GF(Q)$ is the finite field with Q elements and $\mathbb{F}_Q^*$, the multiplication group of $\mathbb{F}_Q$.
- $\mathbb{F}_2^n$ is a vector space over $\mathbb{F}_2 = \{0,1\}$ with a set of all binary n-tuples.
- Let n, m be positive integers and $m|n$. The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is denoted by $Tr_m^n(x)$, i.e.,

$$Tr_m^n(x) = x + x^{2^m} + \cdots + x^{2^{m(\frac{n}{m}-1)}}, x \in \mathbb{F}_{2^n}.$$

  $Tr_1^n(x)$ is simply denoted as $Tr(x)$ if context is clear.

A. Basic concepts

(a) Boolean function

Let $\mathbf{x} = (x_1, \cdots, x_n)$ be a vector in $\mathbb{F}_2^n$ with $x_i \in \mathbb{F}_2$ and $f(\mathbf{x})$ a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then, the function $f(\mathbf{x})$ taking on values 0 or 1 is called a *Boolean function* [11]. A Boolean function consists of a sum of all possible products of x_{i_j}'s [12], i.e.,

$$f(\mathbf{x}) = f(x_1, \cdots, x_n) = \sum c_{i_1 i_2 \cdots i_j} x_{i_1} x_{i_2} \cdots x_{i_j}, \quad c_{i_1 i_2 \cdots i_j} \in \mathbb{F}_2$$

where maximum value of j with nonzero $c_{i_1 i_2 \cdots i_j}$ is called the *degree* of the Boolean function $f(\mathbf{x})$.

(b) Reed-Muller codes

For $0 \le r \le n$, the *rth order Reed-Muller (RM) code* $R(r,n)$ of length $N = 2^n$ is defined by the set of all vectors $F(\mathbf{y}_1, \cdots, \mathbf{y}_n)$ of length N given by [11]

$$F(\mathbf{y}_1, \cdots, \mathbf{y}_n) = c_0\underline{\mathbf{1}} + \sum_{1 \le j \le r} c_{i_1 i_2 \cdots i_j}\mathbf{y}_{i_1} \cdot \mathbf{y}_{i_2} \cdots \mathbf{y}_{i_j}, \quad c_0, c_{i_1 i_2 \cdots i_j} \in \mathbb{F}_2,$$

where $\underline{\mathbf{1}} = (1, \cdots, 1)$ of length N, $\mathbf{y}_1, \cdots, \mathbf{y}_n$ are basis vectors of length N for $R(1,n)$, $\{i_1, \cdots, i_j\} \subset \{1, 2, \cdots, n\}$, and $\mathbf{y}_i \cdot \mathbf{y}_j$ is the vector whose kth element is the product of kth elements of $\mathbf{y}_i$ and $\mathbf{y}_j$, respectively. Therefore, the kth element of a codeword in $R(r,n)$ is given by a Boolean function $f(y_{1,k}, \cdots, y_{n,k})$ with degree of at most r, where $y_{1,k}, \cdots, y_{n,k}$ are the kth elements of $\mathbf{y}_1, \cdots, \mathbf{y}_n$, respectively. If we remove the kth component corresponding to $y_{1,k} = \cdots = y_{n,k} = 0$, then we obtain a *punctured* RM code $R(r,n)^*$ for $0 \le r \le n-1$, where each codeword has length $2^n - 1$.

(c) Trace representation of a binary periodic sequence

Let $\mathcal{S}$ be the set of all binary sequences with period $t|(2^n - 1)$ and $\mathcal{F}$ be the set of all functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. For any function $f(x) \in \mathcal{F}$, $f(x)$ can be represented as [12]

$$f(x) = \sum_{i=1}^{r} Tr_1^{n_i}(A_i x^{t_i}), \quad A_i \in \mathbb{F}(2^{n_i})$$

where t_i is a coset leader of a cyclotomic coset modulo $2^{n_i} - 1$, and $n_i|n$ is the size of the cyclotomic coset containing t_i. For any sequence $\mathbf{a} = \{a_i\} \in \mathcal{S}$, there exists $f(x) \in \mathcal{F}$ such that

$$a_i = f(\alpha^i), \quad i = 0, 1, \cdots,$$

where α is a primitive element of $\mathbb{F}_{2^n}$. Then, $f(x)$ is called a *trace representation* of $\mathbf{a}$. The linear span of the sequence $\mathbf{a}$ is equal to $\sum_{i, A_i \ne 0} n_i$, or equivalently the degree of the shortest linear feedback shift registers that can generate $\mathbf{a}$.

(d) Weight and exponential sum of a binary codeword or sequence

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{v-1})$ be a binary codeword of length v, or a binary sequence with period v. The number of 1's in the codeword is called a *(Hamming) weight*. Clearly, the total sum of additive character $(-1)^{a_i}$ of a codeword or sequence $\mathbf{a}$ with weight w is given by

$$\sum_{i=0}^{v-1} (-1)^{a_i} = v - 2w.$$

If $v = 2^n - 1$ and $\mathbf{a}$ is represented by a trace representation $f(x)$, i.e., $a_i = f(\alpha^i)$ for a primitive element α of $\mathbb{F}_{2^n}$, then the *exponential sum of* $f(x)$ *over* $\mathbb{F}_{2^n}$ is given by

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} = 1 + \sum_{i=0}^{v-1} (-1)^{a_i} = 2^n - 2w.$$

with $f(0) = 0$. Hence, the exponential sum of a polynomial function $f(x)$ has one-to-one correspondence with the weight of a codeword or sequence given by $f(x)$.

(e) Correlation of binary sequences

Let $\mathbf{a}$ and $\mathbf{b}$ be binary sequences with period v. The correlation of $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i + b_{i+\tau}}, \quad 0 \le \tau \le v-1,$$

where τ is a phase shift of the sequence $\mathbf{b}$ and the indices are reduced modulo v. If $\mathbf{b}$ is shift equivalent to $\mathbf{a}$, i.e., $\mathbf{b} = (a_i, a_{i+1}, \cdots, a_{i-1})$, $C_{\mathbf{a},\mathbf{b}}(\tau)$ is the *autocorrelation* of $\mathbf{a}$, $C_{\mathbf{a}}(\tau)$ for short. Otherwise, $C_{\mathbf{a},\mathbf{b}}(\tau)$ is the *cross correlation* of $\mathbf{a}$ and $\mathbf{b}$. If we write $a_i + b_{i+\tau} = f(\alpha^i)$ for a polynomial function $f(x)$ with a given τ and a primitive element α of $\mathbb{F}_{2^n}$, then

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i + b_{i+\tau}} = -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)}.$$

with $f(0) = 0$. Hence, $C_{\mathbf{a},\mathbf{b}}(\tau)$ can be presented by the exponential sum of $f(x)$.

(f) Binary signal set

For r binary shift distinct sequences with period v, i.e., $\mathbf{s}^{(j)} = (s_0^{(j)}, \cdots, s_{v-1}^{(j)}), 0 \le j < r$, let $\mathcal{S} = \{\mathbf{s}^{(0)}, \cdots, \mathbf{s}^{(r-1)}\}$ and

$$C_{\max} = \max |C_{\mathbf{s}^{(i)},\mathbf{s}^{(j)}}(\tau)| \text{ for any } 0 \le \tau < v, \ 0 \le i, j < r$$

where $\tau \ne 0$ if $i = j$. Clearly, $C_{\max}$ is maximum of all nontrivial auto and cross correlations of sequences. The set $\mathcal{S}$ is called a $(v, r, C_{\max})$ *signal set* or *family of sequences*, where r is called a *set size* or *family size*, and $C_{\max}$ is *maximum correlation* of $\mathcal{S}$.

B. Weight distribution of a linear subcode of $R(2,n)^*$

In this paper, we consider a component-wise sum of a pair of binary sequences, where the sum is equivalent to a codeword of a linear cyclic subcode of a punctured second order Reed-Muller code. Thus, we can apply the weight distribution of the subcode to the distribution of correlation values of the sequences.

(a) Weight distribution of a codeword set with rank $2h$

For odd $n = 2l + 1$, we can consider a codeword given by

$$f(x) = Tr(\eta_0 x) + \sum_{j=1}^{l} Tr(\eta_j x^{1+2^j}), \quad x \in \mathbb{F}_{2^n}^*, \tag{1}$$

where each $\eta_j, 0 \le j \le l$, is an element in $\mathbb{F}_{2^n}$. For even $n = 2l$, on the other hand, we can consider a codeword given by

$$f(x) = Tr(\eta_0 x) + \sum_{j=1}^{l-1} Tr(\eta_j x^{1+2^j}) + Tr_1^l(\eta_l x^{1+2^l}), \quad x \in \mathbb{F}_{2^n}^*, \tag{2}$$

where each $\eta_j \in \mathbb{F}_{2^n}$ for $0 \le j \le l-1$, and $\eta_l \in \mathbb{F}_{2^l}$. With respect to a basis $\{\gamma_1, \cdots, \gamma_n\}$ of $\mathbb{F}_{2^n}$, $x = \sum_{i=1}^{n} x_i \gamma_i$ is the expansion of x with $x_i \in \mathbb{F}_2$ for all i. Applying this expansion to (1) or (2), we see that $f(x) = f\left(\sum_{i=1}^{n} x_i \gamma_i\right)$ is equivalent to a Boolean function of degree less than or equal to 2, a *quadratic Boolean function* [13], and it may be written as follows:

$$f(\mathbf{x}) = f(x_1, \cdots, x_n) = \mathbf{x}\mathbf{Q}\mathbf{x}^t + \mathbf{w} \cdot \mathbf{x}^t, \quad \mathbf{x} \in \mathbb{F}_2^n \setminus \{\underline{\mathbf{0}}\} \tag{3}$$

where $\mathbf{Q}$ is an $n \times n$ binary upper triangular matrix, $\mathbf{w}$ is a binary vector in $\mathbb{F}_2^n$, and $\underline{\mathbf{0}} = (0, \cdots, 0)$ is a zero vector of length n. Obviously, $\mathbf{Q}$ is determined by η_j's for nonzero j, and $\mathbf{w}$ by η_0. While $\mathbf{x} = (x_1, \cdots, x_n)$ runs through each nonzero binary n-tuple in $\mathbb{F}_2^n$, $f(\mathbf{x})$ produces each element of a codeword of length $2^n - 1$ in $R(2,n)^*$. Equivalently, $f(x)$ forms a codeword in $R(2,n)^*$ for $x \in \mathbb{F}_{2^n}^*$.

For a given nonzero $\mathbf{Q}$, it is well known that the weight distribution of corresponding set of codewords of $f(\mathbf{x})$ for all $\mathbf{w}$ is determined by a rank of the *symplectic matrix* $\mathbf{B} = \mathbf{Q} + \mathbf{Q}^t$ [11]. Equivalently, we can consider the *symplectic form* $B_f(x,z) = f(x) + f(x+z) + f(z)$ associated with $f(x)$ for given η_j's, $1 \le j \le l$ [13] [14]. We list the following fact regarding the distribution of exponential sums of $f(x)$.

Fact 1 (Theorem 6.2 in [13]): Let η_j's of $f(x)$ in (1) or (2) be given such that at least one η_j is nonzero for $1 \le j \le l$, where $l = \lfloor \frac{n}{2} \rfloor$. For an integer h, $1 \le h \le l$, if $f(x)$ has a rank $2h$, or equivalently $B_f(x,z) = 0$ has 2^{n-2h} solutions of $x \in \mathbb{F}_{2^n}$ for all $z \in \mathbb{F}_{2^n}^*$, then the exponential sums of $f(x)$ have values of 0 and $\pm 2^{n-h}$ for all $\eta_0 \in \mathbb{F}_{2^n}$, and its distribution is given by

$$\sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)} = \begin{cases} 0, & 2^n - 2^{2h} \text{ times} \\ +2^{n-h}, & 2^{2h-1} + 2^{h-1} \text{ times} \\ -2^{n-h}, & 2^{2h-1} - 2^{h-1} \text{ times} \end{cases}$$

with $f(0) = 0$.

(b) Weight distribution of a linear subcode with multiple ranks

For a set of distinct nonzero $\mathbf{Q}$'s, we can consider a set of codewords given by $f(\mathbf{x})$ in (3) for all $\mathbf{w}$. Equivalently, we can consider a set of codewords given by $f(x)$ for distinct sets of η_j's such that in each set of η_j's, at least one η_j is nonzero for $1 \le j \le l$. Then, $f(x)$ may have distinct multiple ranks each of which corresponds to each set of given η_j's. Consequently, the exponential sums of $f(x)$ can take 0 and $\pm 2^{n-h}$ for each possible h from Fact 1. If $f(x)$ further constitutes a linear subcode C_S for the sets of η_j's, we can use the weight distributions of C_S in order to investigate the distribution of exponential sums of $f(x)$. With given weights of a linear code, we can obtain its distribution which is determined by its codeword length, dimension, and the number of distinct weights [11]. Finally, the distribution can be used to investigate the distribution of correlation values of binary sequences, where the correlation corresponds to the exponential sum of $f(x)$.

Next, we specify the known weight distributions of two linear cyclic subcodes of $R(2,n)^*$ for odd n, which will be used in a later section for determining the distribution of correlation values of a new family of sequences. For a, b in $\mathbb{F}_{2^n}$ and k with $\gcd(k,n) = 1$ for odd n, a linear cyclic subcode C_G given by $f(x) = Tr(ax) + Tr(bx^{2^k+1})$ for $x \in \mathbb{F}_{2^n}^*$ has the distribution of weights and corresponding exponential sums in Table I. In Table I, $h = \frac{n-1}{2}$. For a, b, c in $\mathbb{F}_{2^n}$ for odd n, a linear cyclic subcode C_T given by $f(x) = Tr(ax) + Tr(bx^3) + Tr(cx^5)$ for $x \in \mathbb{F}_{2^n}^*$ has the distribution of weights and corresponding exponential sums in Table II. In both Tables, the exponential sum means $\sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)}$ with $f(0) = 0$. There are several different ways to establish the validity of weight distribution of C_G, for example, see [6] and [11]. For those of C_T, see [11].

III. New family of binary sequences with large size

In this section, we present new families of binary sequences with large family size as well as large linear span for odd and even n.

TABLE I

WEIGHT DISTRIBUTION OF C_G GIVEN BY $f(x) = Tr(ax) + Tr(bx^{2^k+1})$

Weight	Exponential Sum	Distribution
0	2^n	1
$2^{n-1} - 2^{n-h-1}$	2^{n-h}	$(2^n - 1)(2^{2h-1} + 2^{h-1})$
2^{n-1}	0	$(2^n - 1)(2^n - 2^{2h} + 1)$
$2^{n-1} + 2^{n-h-1}$	-2^{n-h}	$(2^n - 1)(2^{2h-1} - 2^{h-1})$

TABLE II

WEIGHT DISTRIBUTION OF C_T GIVEN BY $f(x) = Tr(ax) + Tr(bx^3) + Tr(cx^5)$

Weight	Exponential Sum	Distribution
0	2^n	1
$2^{n-1} \pm 2^{\frac{n+1}{2}}$	$\mp 2^{\frac{n+3}{2}}$	$\frac{1}{3}(2^n - 1) \cdot 2^{\frac{n-5}{2}} \cdot (2^{\frac{n-3}{2}} \mp 1) \cdot (2^{n-1} - 1)$
2^{n-1}	0	$(2^n - 1) \cdot (9 \cdot 2^{2n-4} + 3 \cdot 2^{n-3} + 1)$
$2^{n-1} \pm 2^{\frac{n-1}{2}}$	$\mp 2^{\frac{n+1}{2}}$	$\frac{1}{3}(2^n - 1) \cdot 2^{\frac{n-3}{2}} \cdot (2^{\frac{n-1}{2}} \mp 1) \cdot (5 \cdot 2^{n-1} + 4)$

A. Construction of $\mathcal{S}_o(\rho)$ for odd n

Construction 1: For odd $n = 2l + 1$ and an integer ρ, $1 \le \rho \le l$, a family $\mathcal{S}_o(\rho)$ of binary sequences is defined by

$$\mathcal{S}_o(\rho) = \{\mathbf{s}^{\mathbf{\Lambda}} \mid \mathbf{\Lambda} = (\lambda_0, \cdots, \lambda_{\rho-1}),\ \lambda_i \in \mathbb{F}_{2^n}\}$$

where $\mathbf{s}^{\mathbf{\Lambda}} = \{s_0^{\mathbf{\Lambda}}, s_1^{\mathbf{\Lambda}}, \cdots, s_{2^n-2}^{\mathbf{\Lambda}}\}$ is a binary sequence of period $2^n - 1$ with $s_k^{\mathbf{\Lambda}} = s_{\mathbf{\Lambda}}(\alpha^k)$ for a primitive element α of $\mathbb{F}_{2^n}$, where $s_{\mathbf{\Lambda}}(x)$, the trace representation of $s_k^{\mathbf{\Lambda}}$, is given by

$$s_{\mathbf{\Lambda}}(x) = s_{\lambda_0, \cdots, \lambda_{\rho-1}}(x) = Tr(\lambda_0 x) + \sum_{i=1}^{\rho-1} Tr(\lambda_i x^{1+2^i}) + \sum_{i=\rho}^{l} Tr(x^{1+2^i}), \quad x \in \mathbb{F}_{2^n}^*. \qquad (4)$$

The parameters of a new signal set $\mathcal{S}_o(\rho)$ are determined by the following Theorem.

Theorem 1: For odd $n = 2l + 1$ and an integer ρ, $1 \le \rho \le l$, the family $\mathcal{S}_o(\rho)$ has $2^{n\rho}$ shift distinct binary sequences with period $2^n - 1$. The correlation of sequences is $(2\rho + 2)$-valued and maximum correlation is $1 + 2^{\frac{n+2\rho-1}{2}}$. Therefore, $\mathcal{S}_o(\rho)$ constitutes a $(2^n - 1, 2^{n\rho}, 1 + 2^{\frac{n+2\rho-1}{2}})$ signal set.

In order to show Theorem 1, i.e., to determine the family size and correlation of $\mathcal{S}_o(\rho)$, we need the following Lemmas.

Lemma 1: All sequences in $\mathcal{S}_o(\rho)$ are shift distinct. Thus, the family size of $\mathcal{S}_o(\rho)$ is $2^{n\rho}$.

Proof: Consider a time shift version of one sequence represented by

$$s_{\mathbf{\Theta}}(\delta x) = Tr(\theta_0 \delta x) + \sum_{i=1}^{\rho-1} Tr(\theta_i \delta^{1+2^i} x^{1+2^i}) + \sum_{i=\rho}^{l} Tr(\delta^{1+2^l} x^{1+2^i})$$

for $\mathbf{\Theta} = (\theta_0, \cdots, \theta_{\rho-1})$, $\theta_i \in \mathbb{F}_{2^n}$, and $\delta \in \mathbb{F}_{2^n}^*$. It is identical to another sequence of (4), i.e., $s_{\mathbf{\Lambda}}(x) = s_{\mathbf{\Theta}}(\delta x)$ for all x in $\mathbb{F}_{2^n}^*$ if and only if

$$\lambda_0 = \theta_0 \delta, \ \lambda_i = \theta_i \delta^{1+2^i} \text{ for } 1 \le i < \rho, \text{ and } \delta^{1+2^i} = 1 \text{ for } \rho \le i \le l. \tag{5}$$

From $\gcd(2^n - 1, 1 + 2^{\frac{n-1}{2}}) = 1$ for odd n, $\delta = 1$ is a unique solution achieving $\delta^{1+2^l} = 1$. If $\delta = 1$ in (5), it only gives a trivial solution of $\lambda_i = \theta_i$ for $0 \le i < \rho$. Thus, sequences in $\mathcal{S}_o(\rho)$ represented by $s_{\mathbf{\Lambda}}(x)$ for any λ_i in $\mathbb{F}_{2^n}, 0 \le i < \rho$, are shift-distinct. ■

The cross correlation of the two sequences $\mathbf{s}^{\mathbf{\Lambda}}$ and $\mathbf{s}^{\mathbf{\Theta}}$ in $\mathcal{S}_o(\rho)$ is given by

$$C_{\mathbf{s}^{\mathbf{\Lambda}},\mathbf{s}^{\mathbf{\Theta}}}(\tau) = -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)}$$

where

$$f(x) = Tr(\eta_0 x) + \sum_{i=1}^{l} Tr(\eta_i x^{1+2^i}) \tag{6}$$

where

$$\eta_i = \begin{cases} \lambda_0 + \theta_0 \delta, & i = 0 \\ \lambda_i + \theta_i \delta^{1+2^i}, & 1 \le i < \rho \\ 1 + \delta^{1+2^i}, & \rho \le i \le l \end{cases} \tag{7}$$

for $\lambda_i, \theta_i, 0 \le i < \rho$, in $\mathbb{F}_{2^n}$ and $\delta \in \mathbb{F}_{2^n}^*$. In other words, the sum of the sequence $\mathbf{s}^{\mathbf{\Lambda}}$ and τ shift of the sequence $\mathbf{s}^{\mathbf{\Theta}}$ can be considered as a codeword given by $f(x)$ defined by (6). Thus, we only need to investigate the exponential sum of $f(x)$ for the correlation of a pair of the sequences. In the following, we classify the exponential sums in terms of values of η_i.

Case 1. $\eta_i = 0$ for $0 \le i \le l$. In this case, $f(x) = 0$. This corresponds to a trivial exponential sum corresponding to in-phase autocorrelation of a sequence. Clearly, its exponential sum is 2^n.

Case 2. $\eta_0 \neq 0$ and $\eta_i = 0$ for $1 \leq i \leq l$. In this case, $f(x) = Tr(\eta_0 x)$. Hence, we have the exponential sum 0 for any $\eta_0 \in \mathbb{F}_{2^n}^*$, from the orthogonality of a trace function [12].

Case 3. At least one $\eta_i \neq 0$ for $1 \leq i \leq l$. In this case, $f(x)$ is equivalent to a quadratic Boolean function. Thus, we need to investigate the number of roots of its symplectic form $B_f(x,z)$ in order to apply Fact 1 for determining the distribution of the exponential sums of $f(x)$.

Lemma 2: For odd $n = 2l+1$ and an integer $\rho, 1 \leq \rho \leq l$, let η_i's of $f(x)$ be given such that at least one η_i is nonzero for $1 \leq i \leq l$. Then, the symplectic form $B_f(x,z)$ associated with $f(x)$ has at most $2^{2\rho-1}$ roots in $\mathbb{F}_{2^n}$.

Proof: For given η_i's, the symplectic form $B_f(x,z)$ associated with $f(x)$ is given by

$$\begin{aligned} B_f(x,z) &= f(x)+f(x+z)+f(z) \\ &= \sum_{i=1}^{l} Tr\left(\eta_i(xz^{2^i}+x^{2^i}z)\right) \\ &= Tr\left(z\sum_{i=1}^{l}(\eta_i^{2^{-i}}x^{2^{-i}}+\eta_i x^{2^i})\right) = Tr\left(zL(x)\right). \end{aligned}$$

For all $z \in \mathbb{F}_{2^n}^*$, $B_f(x,z) = 0$ if and only if $L(x) = 0$. From (7),

$$\begin{aligned} L(x) &= \sum_{i=1}^{\rho-1}(\eta_i^{2^{-i}}x^{2^{-i}}+\eta_i x^{2^i}) + \sum_{i=\rho}^{l}((1+\delta^{1+2^{-i}})x^{2^{-i}}+(1+\delta^{1+2^i})x^{2^i}) \\ &= \sum_{i=1}^{\rho-1}(\eta_i^{2^{-i}}x^{2^{-i}}+\eta_i x^{2^i}) + \sum_{i=1}^{\rho-1}((1+\delta^{1+2^{-i}})x^{2^{-i}}+(1+\delta^{1+2^i})x^{2^i}) \\ &\quad + \sum_{i=1}^{l}((1+\delta^{1+2^{-i}})x^{2^{-i}}+(1+\delta^{1+2^i})x^{2^i}) \\ &= \sum_{i=1}^{\rho-1}((\eta_i^{2^{-i}}+1+\delta^{1+2^{-i}})x^{2^{-i}}+(\eta_i+1+\delta^{1+2^i})x^{2^i}) + \sum_{i=1}^{n-1}(1+\delta^{1+2^i})x^{2^i}. \end{aligned}$$

Note that

$$\begin{aligned} \sum_{i=1}^{n-1}(1+\delta^{1+2^i})x^{2^i} &= \sum_{i=1}^{n-1}x^{2^i}+\delta\sum_{i=1}^{n-1}(\delta x)^{2^i} \\ &= x+Tr(x)+\delta(Tr(\delta x)+\delta x) \\ &= (1+\delta^2)x+Tr(x)+\delta Tr(\delta x). \end{aligned} \tag{8}$$

Let

$$\gamma_i = \eta_i + 1 + \delta^{1+2^i}. \tag{9}$$

Then, we have $\gamma_i^{2^{-i}} = \eta_i^{2^{-i}} + 1 + \delta^{1+2^{-i}}$. Together with (8),

$$L(x) = q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) + Tr(x) + \delta Tr(\delta x),$$

where

$$q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) = (1+\delta^2)x + \sum_{i=1}^{\rho-1}(\gamma_i^{2^{-i}}x^{2^{-i}} + \gamma_i x^{2^i}). \tag{10}$$

For $L(x) = 0$, we have to count the number of solutions in the equation

$$q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) + Tr(x) + \delta Tr(\delta x) = 0 \tag{11}$$

for given γ_i's in $\mathbb{F}_{2^n}$ and δ in $\mathbb{F}_{2^n}^*$.

Next, we verify that $q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x)$ is a nontrivial polynomial of x considering its coefficients. If $\delta = 1$, $\gamma_i = \eta_i$ for $1 \le i < \rho$, and $\eta_i = 0$ for $\rho \le i \le l$. Then, at least one γ_i is nonzero for $1 \le i < \rho$ because at least one η_i is nonzero. If $\delta \neq 1$, on the other hand, $(1+\delta^2)$ cannot be zero although γ_i may be zero for all $1 \le i < \rho$. Therefore, $q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x)$ is a polynomial of x with at least one nonzero coefficient of x^{2^i} for $-\rho < i < \rho$.

For the nontrivial polynomial $q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x)$, the equation in (11) can be divided into four classes.

i) $Tr(x) = 0$ and $Tr(\delta x) = 0 \;\Rightarrow\; q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) = 0$.

ii) $Tr(x) = 0$ and $Tr(\delta x) = 1 \;\Rightarrow\; q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) + \delta = 0$.

iii) $Tr(x) = 1$ and $Tr(\delta x) = 0 \;\Rightarrow\; q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) + 1 = 0$.

iv) $Tr(x) = 1$ and $Tr(\delta x) = 1 \;\Rightarrow\; q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) + 1 + \delta = 0$.

Thus, the left-hand side of (11) can be presented by

$$A_a(x) = q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) + a = a + (1+\delta^2)x + \sum_{i=1}^{\rho-1}(\gamma_i^{2^{-i}}x^{2^{-i}} + \gamma_i x^{2^i})$$

for $a \in \{0, 1, \delta, 1+\delta\}$. Then,

$$\begin{aligned} A_a^{2^{\rho-1}}(x) &= \left[q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x) + a\right]^{2^{\rho-1}} \\ &= a^{2^{\rho-1}} + (1+\delta^2)^{2^{\rho-1}}x^{2^{\rho-1}} + \sum_{i=1}^{\rho-1}(\gamma_i^{2^{\rho-1-i}}x^{2^{\rho-1-i}} + \gamma_i^{2^{\rho-1}}x^{2^{\rho-1+i}}) \end{aligned}$$

and

$$A_a^{2^{\rho-1}}(x)=0 \;\; \Leftrightarrow A_a(x)=0.$$

Thus, solutions for $A_a^{2^{\rho-1}}(x)=0$ are all solutions for $A_a(x)=0$, and vice versa. Therefore, the number of solutions for $A_a(x)=0$ is equal to that for $A_a^{2^{\rho-1}}(x)=0$. Since the maximum degree of $A_a^{2^{\rho-1}}(x)$ is $2^{2(\rho-1)}$, $A_a^{2^{\rho-1}}(x)=0$ has at most $2^{2(\rho-1)}$ solutions.

If $\delta\neq 1$, the solutions of $A_a^{2^{\rho-1}}(x)=0$ are disjoint for different $a\in\{0,1,\delta,1+\delta\}$, so the total number of solutions of (11) is at most $2^{2(\rho-1)}\cdot 4=2^{2\rho}$. If $\delta=1$, on the other hand, the solutions of $A_a^{2^{\rho-1}}(x)=0$ are disjoint for different $a\in\{0,1\}$, so the total number of solutions of (11) is at most $2^{2(\rho-1)}\cdot 2=2^{2\rho-1}$. From Fact 1, meanwhile, possible number of roots of $B_f(x,z)$ is 2^{n-2h} for a rank $2h$ of $f(x)$, where $n-2h$ is a positive odd integer for odd n. For any value of δ in $\mathbb{F}_{2^n}^*$, therefore, the maximum number of solutions of $B_f(x,z)=0$ is $2^{2\rho-1}$. ■

From (9) in the proof of Lemma 2, since η_i can run through all elements in $\mathbb{F}_{2^n}$, we can set $\eta_i=1+\delta^{1+2^i}$ for i with $k\leq i\leq\rho-1$, where k is a constant with $1\leq k\leq\rho-1$. Then $\gamma_i=0$ for i with $k\leq i\leq\rho-1$. Thus, (10) becomes

$$q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x)=(1+\delta^2)x+\sum_{i=1}^{k-1}(\gamma_i^{2^{-i}}x^{2^{-i}}+\gamma_i x^{2^i}).$$

Following the same procedure as we did in the proof of Lemma 2,

$$q_{\gamma_1,\cdots,\gamma_{\rho-1},\delta}(x)+Tr(x)+\delta Tr(\delta x)=0 \tag{12}$$

has at most $2^{2(k-1)}\cdot 4=2^{2k}$ solutions in $\mathbb{F}_{2^n}$. Since the dimension of (12) should be odd, it has at most 2^{2k-1} solutions for each $k, 1\leq k\leq\rho-1$. From this result, together with Lemma 2, we have established the following Proposition.

Proposition 1: While each η_i of $f(x)$ in (6) runs through all elements in $\mathbb{F}_{2^n}$ with at least one nonzero η_i, the symplectic form $B_f(x,z)$ associated with $f(x)$ has 2^{n-2h} roots for every possible integer h where $n-2h$ is any positive odd integer less than or equal to $2\rho-1$.

Lemma 3: For odd $n=2l+1$ and an integer $\rho, 1\leq\rho\leq l$, let η_i's of $f(x)$ in (6) be given such that at least one η_i is nonzero for $1\leq i\leq l$. For all $\eta_0\in\mathbb{F}_{2^n}$, the exponential sums of $f(x)$ can take values of 0 and $\pm 2^{n-h}$ for an integer h where $n-2h$ is a positive odd integer less than or equal to $2\rho-1$.

Proof: From Lemma 2, $B_f(x,z)=0$ has 2^{n-2h} solutions for an integer h where $n-2h$ is a positive odd integer less than or equal to $2\rho-1$. Consequently, Lemma 3 is true from Fact 1. ■

From Proposition 1 and Lemma 3, we see that while each η_i runs through all elements in $\mathbb{F}_{2^n}$ with at least one nonzero η_i, the exponential sums of $f(x)$ can take values of 0 and $\pm 2^{n-h}$ for every possible integer h where $n-2h$ is any positive odd integer less than or equal to $2\rho-1$. Combining the Cases 1, 2, and 3, we have the following result on the correlation of sequences in $\mathcal{S}_o(\rho)$.

Lemma 4: The correlation of binary sequences in $\mathcal{S}_o(\rho)$ is $(2\rho+2)$-valued and maximum correlation $C_{\max}$ is $1+2^{\frac{n+2\rho-1}{2}}$.

Proof: For a trace representation $s_{\mathbf{\Lambda}}(x)$ of each sequence $\mathbf{s}^{\mathbf{\Lambda}}$ in $\mathcal{S}_o(\rho)$, we can consider the exponential sums of $f(x)$ in (6). First of all, the exponential sums have 2^n and 0 values in Cases 1 and 2. For all η_i's in Case 3, from Proposition 1, the exponential sums of $f(x)$ take 0 and $\pm 2^{n-h}$ for every possible value h achieving $n-2h=1,3,\cdots,2\rho-1$. In this case, the exponential sums take 2ρ nonzero distinct values. Including 2^n and 0, therefore, the overall exponential sums are $(2\rho+2)$-valued. Equivalently, the correlation of sequences in $\mathcal{S}_o(\rho)$ is $(2\rho+2)$-valued. Furthermore, the maximum value for $n-2h$ is determined by $2\rho-1$ from Lemma 3. Thus, $C_{\max}=|-1-2^{n-h}|=1+2^{\frac{n+2\rho-1}{2}}$. ■

Proof of Theorem 1. The results follow directly from Lemma 1 and Lemma 4. ■

Remark 1: If $\rho=1$,

$$s_{\lambda_0}(x)=Tr(\lambda_0 x)+\sum_{i=1}^{l} Tr(x^{1+2^i}),\quad x\in\mathbb{F}_{2^n}^*, \tag{13}$$

which represents the *Gold-like Sequence* introduced by Boztas and Kumar [1]. From Lemma 3, a positive odd integer less than 2ρ is only 1, so $n-2h=1$. Hence, $h=\frac{n-1}{2}$. Finally, Gold-like sequences given by (13) has four-valued correlation, or $\{2^n-1,-1,-1\pm 2^{\frac{n+1}{2}}\}$ for all $\lambda_0\in\mathbb{F}_{2^n}$.

Example 1: If $\rho=2$,

$$s_{\lambda_0,\lambda_1}(x)=Tr(\lambda_0 x)+Tr(\lambda_1 x^3)+\sum_{i=2}^{l} Tr(x^{1+2^i}),\quad x\in\mathbb{F}_{2^n}^* \tag{14}$$

for odd $n \geq 5$. From Lemma 3, $n-2h$ is a positive odd integer less than 4, so $n-2h=1$ and 3. Thus, $h=\frac{n-1}{2}$ and $\frac{n-3}{2}$. From Lemma 4, sequences given by (14) have six-valued correlation, or $\{2^n-1, -1, -1 \pm 2^{\frac{n+1}{2}}, -1 \pm 2^{\frac{n+3}{2}}\}$ for all $\lambda_0, \lambda_1 \in \mathbb{F}_{2^n}$. For sequences represented by $s_{\lambda_0,\lambda_1}(x)$ and $s_{\theta_0,\theta_1}(\delta x)$, corresponding $f(x)$ in (6) can constitute a linear cyclic subcode with five nonzero distinct weights if we assume that δ can be any element in $\mathbb{F}_{2^n}$. The subcode has the same weight distribution as that of C_T in Table II because it has the same codeword length, dimension, and weights with C_T. Hence, the distribution of correlation values of $\mathcal{S}_o(2)$ can be derived from Table II. The details will be discussed in Section IV.

Example 2: If $\rho=3$,

$$s_{\lambda_0,\lambda_1,\lambda_2}(x) = Tr(\lambda_0 x) + Tr(\lambda_1 x^3) + Tr(\lambda_2 x^5) + \sum_{i=3}^{l} Tr(x^{1+2^i}), \quad x \in \mathbb{F}_{2^n}^* \tag{15}$$

for odd $n \geq 7$. Similarly, $h=\frac{n-1}{2}, \frac{n-3}{2}$, and $\frac{n-5}{2}$. From Lemma 4, sequences given by (15) have eight-valued correlation, or $\{2^n-1, -1, -1 \pm 2^{\frac{n+1}{2}}, -1 \pm 2^{\frac{n+3}{2}}, -1 \pm 2^{\frac{n+5}{2}}\}$ for all $\lambda_0, \lambda_1, \lambda_2 \in \mathbb{F}_{2^n}$. Similar to $\rho=2$, $f(x)$ in (6) constitutes a linear cyclic subcode with seven nonzero distinct weights with the assumption that δ can be any element in $\mathbb{F}_{2^n}$. Hence, the distribution of correlation values of $\mathcal{S}_o(3)$ can be determined by the weight distribution of the code using Theorem 2 of Chapter 6 in [11].

B. Construction of $\mathcal{S}_e(\rho)$ for even n

Construction 2: For even $n=2l$ and an integer ρ, $1 \leq \rho < l$, a family $\mathcal{S}_e(\rho)$ of binary sequences is defined by

$$\mathcal{S}_e(\rho) = \{\mathbf{s}^{\mathbf{\Lambda}} \mid \mathbf{\Lambda} = (\lambda_0, \cdots, \lambda_{\rho-1}),\ \lambda_i \in \mathbb{F}_{2^n}\}$$

where $\mathbf{s}^{\mathbf{\Lambda}} = \{s_0^{\mathbf{\Lambda}}, s_1^{\mathbf{\Lambda}}, \cdots, s_{2^n-2}^{\mathbf{\Lambda}}\}$ is a binary sequence of period 2^n-1 with $s_k^{\mathbf{\Lambda}} = s_{\mathbf{\Lambda}}(\alpha^k)$ for a primitive element α of $\mathbb{F}_{2^n}$, where $s_{\mathbf{\Lambda}}(x)$, the trace representation of $s_k^{\mathbf{\Lambda}}$, is given by

$$s_{\mathbf{\Lambda}}(x) = Tr(\lambda_0 x) + \sum_{i=1}^{\rho-1} Tr(\lambda_i x^{1+2^i}) + \sum_{i=\rho}^{l-1} Tr(x^{1+2^i}) + Tr_1^l(x^{1+2^l}), \quad x \in \mathbb{F}_{2^n}^*. \tag{16}$$

Theorem 2: For even $n=2l$ and an integer ρ, $1 \leq \rho < l$, the family $\mathcal{S}_e(\rho)$ has $2^{n\rho}$ shift distinct binary sequences with period 2^n-1. The correlation of sequences is $(2\rho+4)$-valued and maximum correlation is $1+2^{\frac{n}{2}+\rho}$. Therefore, $\mathcal{S}_e(\rho)$ constitutes a $(2^n-1, 2^{n\rho}, 1+2^{\frac{n}{2}+\rho})$ signal set.

In order to prove Theorem 2, we need the following Lemmas. However, the proofs for those Lemmas are similar to those for $\mathcal{S}_o(\rho)$. Hence, we omit the details.

Lemma 5: All sequences in $\mathcal{S}_e(\rho)$ are shift distinct. Hence, the family size of $\mathcal{S}_e(\rho)$ is $2^{n\rho}$.

Proof: Similar to the proof of Lemma 5, $s_{\mathbf{\Lambda}}(x) = s_{\mathbf{\Theta}}(\delta x)$ for all x in $\mathbb{F}_{2^n}^*$ if and only if (5) is achieved. From $\gcd(1+2^{\frac{n}{2}}, 1+2^{\frac{n-2}{2}}) = 1$ for even n, the unique solution of (5) is from $\delta = 1$, resulting in a trivial solution. Hence, all sequences in $\mathcal{S}_e(\rho)$ are shift distinct. ■

To investigate the correlation of sequences in $\mathcal{S}_e(\rho)$, we need to consider $f(x)$ given by

$$f(x) = Tr(\eta_0 x) + \sum_{i=1}^{l-1} Tr(\eta_i x^{1+2^i}) + Tr_1^l(\eta_l x^{1+2^l}) \tag{17}$$

where

$$\eta_i = \begin{cases} \lambda_0 + \theta_0\delta, & i = 0 \\ \lambda_i + \theta_i\delta^{1+2^i}, & 1 \le i < \rho \\ 1 + \delta^{1+2^i}, & \rho \le i \le l \end{cases} \tag{18}$$

for $\lambda_i, \theta_i, 0 \le i < \rho$, in $\mathbb{F}_{2^n}$ and $\delta \in \mathbb{F}_{2^n}^*$. If $\eta_i = 0$ for all $1 \le i \le l$, the exponential sum of $f(x)$ has a value of 0 or 2^n. Otherwise, we have to consider the number of solutions of $B_f(x,z) = 0$ in order to derive the distribution of exponential sums of $f(x)$ in (17).

Lemma 6: For even $n = 2l$ and an integer $\rho, 1 \le \rho < l$, let η_i's of $f(x)$ be given such that at least one η_i is nonzero for $1 \le i \le l$. Then, the symplectic form $B_f(x,z)$ associated with $f(x)$ has at most $2^{2\rho}$ roots in $\mathbb{F}_{2^n}$ (or at most $2^{2\rho-2}$ roots for $\delta = 1$).

Proof: We have

$$B_f(x,z) = Tr\left(z\left(\sum_{i=1}^{l-1}(\eta_i^{2^{-i}} x^{2^{-i}} + \eta_i x^{2^i}) + \eta_l x^{2^l}\right)\right) = Tr\left(zL(x)\right).$$

Thus, $B_f(x,z) = 0$ for all $z \in \mathbb{F}_{2^n}^*$ if and only if $L(x) = 0$. Using the same approach as we did in the proof of Lemma 2, we can obtain equation (11). Following the same steps in the proof of Lemma 2, we can derive that the number of solutions of $B_f(x,z) = 0$ is at most $2^{2\rho}$ (or $2^{2\rho-2}$ for $\delta = 1$). ■

Lemma 7: For even $n = 2l$ and an integer $\rho, 1 \leq \rho < l$, let η_i's of $f(x)$ in (17) be given such that at least one η_i is nonzero for $1 \leq i \leq l$. For all $\eta_0 \in \mathbb{F}_{2^n}$, the exponential sums of $f(x)$ can take values of 0 and $\pm 2^{n-h}$ for an integer h where $n - 2h$ is zero or a positive even integer less than or equal to 2ρ (or $2\rho - 2$ for $\delta = 1$).

Lemma 8: The correlation of binary sequences in $\mathcal{S}_e(\rho)$ is $(2\rho + 4)$-valued and maximum correlation $C_{\max}$ is $1 + 2^{\frac{n}{2}+\rho}$.

Proof: Similar to odd n, we see that while each $\eta_i, 1 \leq i < l$, and η_l run through all elements in $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^l}$ with at least one nonzero η_i, the exponential sums of $f(x)$ can take values of 0 and $\pm 2^{n-h}$ for every possible integer h where $n - 2h$ is zero or any positive even integer less than or equal to 2ρ. Hence, $n - 2h = 0, 2, \cdots, 2\rho$. Consequently, the number of nonzero and nontrivial values of exponential sums is $2(\rho + 1)$. Including 0 and 2^n, the correlation is $(2\rho + 4)$-valued. Furthermore, $C_{\max} = 1 + 2^{\frac{n}{2}+\rho}$ for $h = \frac{n}{2} - \rho$. ■

Proof of Theorem 2. The results follow directly from Lemma 5 and Lemma 8. ■

Remark 2: If $\rho = 1$,

$$s_{\lambda_0}(x) = Tr(\lambda_0 x) + \sum_{i=1}^{l-1} Tr(x^{1+2^i}) + Tr_1^l(x^{1+2^l}), \quad x \in \mathbb{F}_{2^n}^* \tag{19}$$

which represents the sequence constructed by Udaya [2]. From Lemma 7, $n - 2h = 0, 2$. Hence, $h = \frac{n}{2}, \frac{n}{2} - 1$. Finally, the sequences given by (19) has six-valued correlation, or $\{2^n - 1, -1, -1 \pm 2^{\frac{n}{2}}, -1 \pm 2^{\frac{n}{2}+1}\}$ for all $\lambda_0 \in \mathbb{F}_{2^n}$.

Example 3: If $\rho = 2$,

$$s_{\lambda_0,\lambda_1}(x) = Tr(\lambda_0 x) + Tr(\lambda_1 x^3) + \sum_{i=2}^{l} Tr(x^{1+2^i}) + Tr_1^l(x^{1+2^l}), \quad x \in \mathbb{F}_{2^n}^* \tag{20}$$

for even $n \geq 6$. From Lemma 7, $n - 2h = 0, 2, 4$. Thus, $h = \frac{n}{2}, \frac{n}{2} - 1, \frac{n}{2} - 2$. From Lemma 8, sequences given by (20) have eight-valued correlation, or $\{2^n - 1, -1, -1 \pm 2^{\frac{n}{2}}, -1 \pm 2^{\frac{n}{2}+1}, -1 \pm 2^{\frac{n}{2}+2}\}$ for all $\lambda_0, \lambda_1 \in \mathbb{F}_{2^n}$. Contrary to odd case, $f(x)$ in (17) does not constitute a linear cyclic subcode in general because the exponent $1 + 2^i$ may not be coprime with $2^n - 1$ for even n, so that $\eta_i, \rho \leq i \leq l$ may not run through all elements in $\mathbb{F}_{2^n}$ when δ runs through all elements in $\mathbb{F}_{2^n}$. Therefore, we should use different methods from odd n to investigate the distribution of correlation values of sequences in $\mathcal{S}_e(2)$, which is a problem that we are working on.

TABLE III

LINEAR SPAN AND NUMBER OF CORRESPONDING SEQUENCES IN $\mathcal{S}_o(\rho)$ (OR $\mathcal{S}_e(\rho)$)

$LS(\rho)$	Number of sequences
$\frac{n(n+1)}{2}$	$(2^n-1)^\rho$
$\frac{n(n-1)}{2}$	$\binom{\rho}{1}\cdot(2^n-1)^{\rho-1}$
$\frac{n(n-3)}{2}$	$\binom{\rho}{2}\cdot(2^n-1)^{\rho-2}$
$\vdots$	$\vdots$
$\frac{n(n-2\rho+1)}{2}$	1

C. Linear span of $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$

The linear span of a binary sequence in $\mathcal{S}_o(\rho)$ or $\mathcal{S}_e(\rho)$ is determined by the number of nonzero λ_i's, $0 \le i < \rho$.

Theorem 3: In the family $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$), let's consider a sequence represented by $s_{\mathbf{\Lambda}}(x)$ where j λ_i's in $\mathbf{\Lambda} = (\lambda_0, \cdots, \lambda_{\rho-1})$ are equal to 0 for $0 \le i < \rho$. Let $LS_j(\rho)$ be the linear span of such a sequence. Then,

$$LS_j(\rho) = \frac{n(n-2j+1)}{2}, \quad 0 \le j \le \rho$$

and there are $\binom{\rho}{j}\cdot(2^n-1)^{\rho-j}$ sequences in $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$) has linear span $LS_j(\rho)$. From this result, the linear span of sequences in $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$) and their distribution are shown in Table III.

Proof: At first, consider the linear span of sequences in $\mathcal{S}_o(\rho)$. In Construction 1, a sequence represented by $s_{\mathbf{\Lambda}}(x)$ has a total $l+1 = \frac{n+1}{2}$ trace terms and each trace term has linear span of n. If j λ_i's of the sequence are equal to 0, it has $(\frac{n+1}{2}-j)$ nonzero trace terms and corresponding linear span of the sequence is

$$LS_j(\rho) = \left(\frac{n+1}{2}-j\right)\cdot n = \frac{n(n-2j+1)}{2}, \quad 0 \le j \le \rho.$$

Since j λ_i's are 0 and $(\rho-j)$ λ_i's are nonzero, the number of corresponding sequences given by $s_{\mathbf{\Lambda}}(x)$ is $\binom{\rho}{j}\cdot(2^n-1)^{\rho-j}$. Applying this result to each j, $0 \le j \le \rho$, we obtain the linear span $LS(\rho)$ of binary sequences in $\mathcal{S}_o(\rho)$ with the distribution in Table III. Using the similar approach to odd case, we see that the linear span of sequences in $\mathcal{S}_e(\rho)$ is the same as $\mathcal{S}_o(\rho)$. ■

TABLE IV

COMPARISON OF THE FAMILIES OF BINARY SEQUENCES WITH LOW CORRELATION

Family of Sequences	Period	Family Size	$C_{\max}$	Maximum Linear Span	n
Gold	2^n-1	2^n+1	$1+2^{\frac{n+1}{2}}$	$2n$	odd
Kasami (Small Set)	2^n-1	$2^{\frac{n}{2}}$	$1+2^{\frac{n}{2}}$	$\frac{3n}{2}$	even
Kasami (Large Set)	2^n-1	$2^{\frac{n}{2}}(2^n+1)-1$	$1+2^{\frac{n}{2}+1}$	$\frac{5n}{2}$	even
		or $2^{\frac{n}{2}}(2^n+1)$			
Bent	2^n-1	$2^{\frac{n}{2}}$	$1+2^{\frac{n}{2}}$	$\sum_{i=1}^{n/4}\binom{n}{i}$	even ($n=4l$)
Boztas and Kumar, Gold-like [1]	2^n-1	2^n+1	$1+2^{\frac{n+1}{2}}$	$\frac{n(n+1)}{2}$	odd
Udaya [2]	2^n-1	2^n+1	$1+2^{\frac{n}{2}+1}$	$\frac{n(n+1)}{2}$	even
Chang *et al.* [9] and triplet code [11]	2^n-1	2^{2n}	$1+2^{\frac{n+3}{2}}$	$3n$	odd
New Family $\mathcal{S}_o(2)$	2^n-1	2^{2n}	$1+2^{\frac{n+3}{2}}$	$\frac{n(n+1)}{2}$	odd
New Family $\mathcal{S}_e(2)$	2^n-1	2^{2n}	$1+2^{\frac{n}{2}+2}$	$\frac{n(n+1)}{2}$	even
New Family $\mathcal{S}_o(\rho), 1<\rho\leq\frac{n-1}{2}$	2^n-1	$2^{n\rho}$	$1+2^{\frac{n+2\rho-1}{2}}$	$\frac{n(n+1)}{2}$	odd
New Family $\mathcal{S}_e(\rho), 1<\rho<\frac{n}{2}$	2^n-1	$2^{n\rho}$	$1+2^{\frac{n}{2}+\rho}$	$\frac{n(n+1)}{2}$	even

Corollary 1: The maximum and minimum linear spans of sequences in $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$ are $\frac{n(n+1)}{2}$ and $\frac{n(n-2\rho+1)}{2}$, respectively.

D. Comparison of families of binary sequences

In Table IV, we give some comparisons of the families $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$ with the well known families of binary sequences with low correlation. In Table IV, we include a family of binary sequences which can be constructed from Chang *et al.*'s investigation of a binary cyclic code based on three-term sequences [9]. For odd $n=2l+1$, each sequence in the family is represented by

$$s_{\lambda_0,\lambda_1}(x)=Tr(\lambda_0 x)+Tr(\lambda_1 x^r)+Tr(x^{r^2}), \quad r=2^{l+1}+1, \ x\in\mathbb{F}_{2^n}^*$$

for all λ_0,λ_1 in $\mathbb{F}_{2^n}$. On the other hand, a family of sequences defined by $s_{\lambda_0,\lambda_1}(x)=Tr(\lambda_0 x)+Tr(\lambda_1 x^3)+Tr(x^5)$ from a triplet code, has the same period, family size, $C_{\max}$, and maximum linear span with Chang *et al.*'s for all λ_0,λ_1 in $\mathbb{F}_{2^n}$ for odd n [11].

In terms of period and maximum linear span, new families $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$ are identical to the families of Gold-like sequences and sequences constructed by Udaya, respectively. At the expense of maximum correlation $C_{\max}$, however, we have larger family size in $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$ than the families of Gold-like sequences and Udaya's construction. Basically, we can obtain new families $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$ of binary sequences of exponentially increased family size with linear increase of $C_{\max}$ from the optimal correlation. Furthermore, we can choose ρ and corresponding family $\mathcal{S}_o(\rho)$ or $\mathcal{S}_e(\rho)$ for its specific application. For example, if low correlation is more crucial than large family size in the application, then a small value of ρ can be chosen. Otherwise, we can choose a large value of ρ in order to get large family size.

IV. Distribution of correlation values of $\mathcal{S}_o(2)$

In many applications, a family of binary sequences with both low correlation and large family size is required. Thus, we need to consider a family of sequences which can be good compromise between correlation and family size. As a good candidate of such a family, we extensively discuss a new sequence family $\mathcal{S}_o(2)$ by analyzing its distribution of correlation values.

For odd $n = 2l+1$, a family $\mathcal{S}_o(2)$ of binary sequences is given by

$$\mathcal{S}_o(2) = \{\mathbf{s}^{\mathbf{\Lambda}} \mid \mathbf{\Lambda} = (\lambda_0, \lambda_1),\ \lambda_i \in \mathbb{F}_{2^n}\}$$

where $\mathbf{s}^{\mathbf{\Lambda}} = \{s_0^{\mathbf{\Lambda}}, s_1^{\mathbf{\Lambda}}, \cdots, s_{2^n-2}^{\mathbf{\Lambda}}\}$ is a binary sequence of period 2^n-1 with $s_k^{\mathbf{\Lambda}} = s_{\lambda_0,\lambda_1}(\alpha^k)$ for a primitive element α of $\mathbb{F}_{2^n}$, where $s_{\lambda_0,\lambda_1}(x)$ is given by

$$s_{\lambda_0,\lambda_1}(x) = Tr(\lambda_0 x) + Tr(\lambda_1 x^3) + \sum_{i=2}^{l} Tr(x^{1+2^i}), \quad x \in \mathbb{F}_{2^n}^{*}.$$

From Theorem 1, we know that the family $\mathcal{S}_o(2)$ has 2^{2n} shift distinct binary sequences with period 2^n-1. The correlation of sequences in $\mathcal{S}_o(2)$ is six-valued and its maximum is $1+2^{\frac{n+3}{2}}$. Consequently, $\mathcal{S}_o(2)$ constitutes a $(2^n-1, 2^{2n}, 1+2^{\frac{n+3}{2}})$ signal set. These data of $\mathcal{S}_o(2)$ are listed in Table IV.

Next, we will investigate the distribution of the correlation values of sequences in $\mathcal{S}_o(2)$. The correlation of a pair of sequences in $\mathcal{S}_o(2)$ is derived from the exponential sum of

$$f(x) = Tr((\lambda_0 + \theta_0\delta)x) + Tr((\lambda_1 + \theta_1\delta^3)x^3) + \sum_{i=2}^{l} Tr((1+\delta^{1+2^i})x^{1+2^i}), \quad x \in \mathbb{F}_{2^n}^{*}$$

for $\lambda_0, \lambda_1, \theta_0, \theta_1 \in \mathbb{F}_{2^n}$ and $\delta \in \mathbb{F}_{2^n}^{*}$. With $a = \lambda_0 + \theta_0\delta, b = \lambda_1 + \theta_1\delta^3$, and $c_i = 1 + \delta^{1+2^i}$ for $2 \le i \le l$, $f(x)$ has a form of

$$f(x) = Tr(ax) + Tr(bx^3) + \sum_{i=2}^{l} Tr(c_i x^{1+2^i}), \quad x \in \mathbb{F}_{2^n}^{*} \tag{21}$$

for $a, b \in \mathbb{F}_{2^n}$ and $c_i \in \mathbb{F}_{2^n} \setminus \{1\}$. Depending on c_i's, the exponential sums of $f(x)$ can be classified into two exclusive cases. To facilitate the analysis, let's assume that c_i can be any element in $\mathbb{F}_{2^n}$.

Case 1. $c_i = 0$ for $2 \leq i \leq l$. In this case, $f(x) = Tr(ax) + Tr(bx^3)$ constitutes a linear cyclic subcode of $R(2, n)^*$ for $a, b \in \mathbb{F}_{2^n}$. Thus, the distribution of the exponential sums of $f(x)$ is identical to Table I with $h = h_1$, where $h_1 = \frac{n-1}{2}$.

Case 2. At least one $c_i \neq 0$ for $2 \leq i \leq l$. In this case, the distribution of the exponential sums of $f(x)$ follows from the following Lemma.

Lemma 9: For given c_i's with at least one nonzero c_i, $f(x)$ in (21) has five valued exponential sums for all a, b in $\mathbb{F}_{2^n}$, and the distribution is

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} = \begin{cases} \pm 2^{n-h_1}, & d_1 \cdot (2^{2h_1-1} \pm 2^{h_1-1}) \text{ times} \\ 0, & d_1 \cdot (2^n - 2^{2h_1}) + d_2 \cdot (2^n - 2^{2h_2}) \text{ times} \\ \pm 2^{n-h_2}, & d_2 \cdot (2^{2h_2-1} \pm 2^{h_2-1}) \text{ times} \end{cases} \tag{22}$$

where $h_1 = \frac{n-1}{2}, h_2 = \frac{n-3}{2}$, and d_1, d_2 are integers such that $d_1 + d_2 = 2^n$.

Proof: If b is fixed to an element in $\mathbb{F}_{2^n}$, the exponential sums of $f(x)$ follows the distribution in Fact 1 depending on its rank. Since $\rho = 2$, it is obvious that $f(x)$ with at least one nonzero c_i may have a pair of distinct ranks $2h_1$ and $2h_2$ depending on b, where $n - 2h_1 = 1$ and $n - 2h_2 = 3$, respectively. For a subset Ω of $\mathbb{F}_{2^n}$, let's assume that if $b \in \Omega$, $f(x)$ has rank $2h_1$ and otherwise, $f(x)$ has rank $2h_2$, where $|\Omega| = d_1$ and $|\Omega^c| = d_2 = 2^n - d_1$. If b runs through all elements in $\mathbb{F}_{2^n}$, the overall distribution of the exponential sum becomes (22) after summing up the distributions for h_1 and h_2. ■

By combining both Cases 1 and 2, we see that $f(x)$ has six-valued exponential sum for any c_i in $\mathbb{F}_{2^n}$. Furthermore, $f(x)$ equivalently constitutes a linear cyclic subcode of $R(2, n)^*$ with five nonzero distinct weights for a, b, and c_i's in $\mathbb{F}_{2^n}$ with the assumption that each c_i determined by δ can be any element in $\mathbb{F}_{2^n}$. Hence, each codeword in the subcode has length $2^n - 1$ and its dimension is $3n$ due to a, b, and δ in $\mathbb{F}_{2^n}$. Since its codeword length, dimension, and weights are the same as those of C_T in Table II, it has the weight distribution of Table II. Using this fact, we can derive values of d_1 and d_2 in Lemma 9.

Lemma 10: For d_1 and d_2 in Lemma 9,

$$d_1 = \frac{1}{3} \cdot (5 \cdot 2^{n-1} + 1), \quad d_2 = \frac{1}{3} \cdot (2^{n-1} - 1).$$

Proof: For given c_i's with at least one nonzero c_i, the exponential sums of $f(x)$ have the distribution of (22). If $c_i = 0$ for $2 \leq i \leq l$, on the other hand, $f(x) = Tr(ax) + Tr(bx^3)$. In this case, the exponential sums of $f(x)$ have the distribution of Table I for $h = h_1 = \frac{n-1}{2}$. By summing up the distributions of both cases, the overall distribution of the exponential sums of $f(x)$ is given by

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)}$$

$$= \begin{cases} 2^n, & 1 \text{ time} \\ \pm 2^{n-h_1}, & (2^n - 1) \cdot (d_1 + 1) \cdot (2^{2h_1 - 1} \pm 2^{h_1 - 1}) \text{ times} \\ 0, & (2^n - 1) \cdot (d_1 \cdot (2^n - 2^{2h_1}) + d_2 \cdot (2^n - 2^{2h_2}) + 2^n - 2^{2h_1} + 1) \text{ times} \\ \pm 2^{n-h_2}, & (2^n - 1) \cdot d_2 \cdot (2^{2h_2 - 1} \pm 2^{h_2 - 1}) \text{ times} \end{cases} \tag{23}$$

for all sets of c_i's in $\mathbb{F}_{2^n}$. However, this distribution is identical to the weight distribution of Table II. Note that $h_1 = \frac{n-1}{2}, h_2 = \frac{n-3}{2}$. Compared with Table II, the values of d_1 and d_2 follow immediately. ■

So far, we assume that c_i can be any element in $\mathbb{F}_{2^n}$. In sequences' aspect, however, c_i's in (21) cannot be 1 with nonzero δ. Thus, we must remove the case from the distribution in (23) in order to obtain the distribution of correlation values of sequences in $\mathcal{S}_o(2)$.

Theorem 4: The complete distribution of correlation values of any pair of binary sequences in $\mathcal{S}_o(2)$ is as follows.

$$C_{\mathbf{s}^{\mathbf{\Lambda}}, \mathbf{s}^{\mathbf{\Lambda}'}} = \begin{cases} 2^n - 1, & 2^{2n} \text{ times} \\ -1 \pm 2^{\frac{n+1}{2}}, & \frac{1}{3} \cdot 2^{2n} \cdot 2^{\frac{n-3}{2}} \cdot (2^{\frac{n-1}{2}} \pm 1) \cdot (5 \cdot 2^{2n-1} - 2^n - 5) \text{ times} \\ -1, & 2^{2n} \cdot (9 \cdot 2^{3n-4} - 3 \cdot 2^{2n-2} + 3 \cdot 2^{n-2} - 1) \text{ times} \\ -1 \pm 2^{\frac{n+3}{2}}, & \frac{1}{3} \cdot 2^{2n} \cdot 2^{\frac{n-3}{2}} \cdot (2^{\frac{n-3}{2}} \pm 1) \cdot (2^{n-1} - 1)^2 \text{ times} \end{cases} \tag{24}$$

Proof: (23) shows the distribution of the exponential sums of $f(x)$ for all a, b, and c_i's in $\mathbb{F}_{2^n}$. To investigate the distribution of correlation values of sequences in $\mathcal{S}_o(2)$, we need to consider the distribution of the exponential sums of $f(x)$ without $c_i = 1(\delta = 0)$, which means removing the distribution of (22) from (23). Moreover, note that with respect to the correlation of sequences, a and b run through all elements in $\mathbb{F}_{2^n}$ by θ_0 and θ_1 as well as λ_0 and λ_1, respectively. By additionally multiplying each distribution of exponential sums by 2^{2n}, therefore, we can get the distribution of correlation values of (24). ■

From Theorem 3, the linear span of sequences in $\mathcal{S}_o(2)$ has the following distribution.

$$LS(2) = \begin{cases} \frac{n(n+1)}{2}, & (2^n-1)^2 \text{ times} \\ \frac{n(n-1)}{2}, & 2\cdot(2^n-1) \text{ times} \\ \frac{n(n-3)}{2}. & 1 \text{ time} \end{cases}$$

V. Conclusion and some observations

New families of binary sequences with period 2^n-1 have been presented in this paper. For odd $n = 2l+1$ and an integer $\rho, 1 \le \rho \le l$, a new family $\mathcal{S}_o(\rho)$ has family size of $2^{n\rho}$ and maximum correlation of $1+2^{\frac{n+2\rho-1}{2}}$. For even $n = 2l$ and an integer $\rho, 1 \le \rho < l$, on the other hand, a new family $\mathcal{S}_e(\rho)$ has family size of $2^{n\rho}$ and maximum correlation of $1+2^{\frac{n}{2}+\rho}$. The maximum linear span of both $\mathcal{S}_o(\rho)$ and $\mathcal{S}_e(\rho)$ is $\frac{n(n+1)}{2}$. For each ρ with $1 < \rho \le l$, $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$) contains $\mathcal{S}_o(\rho-1)$ (or $\mathcal{S}_e(\rho-1)$) as a subset. Thus, the new family contains Boztas and Kumar's case corresponding to $\mathcal{S}_o(1)$ (or Udaya's case corresponding to $\mathcal{S}_e(1)$) as a subset if m-sequences are excluded from both cases. The family $\mathcal{S}_o(2)$ is considered as a good candidate with large family size as well as low correlation. For $\mathcal{S}_o(2)$, we further derived the distribution of correlation values of sequences in $\mathcal{S}_o(2)$. For distribution of correlation values of $\mathcal{S}_e(2)$, this is an unsolved problem which we are working on.

At last, we would like to point it out one interesting phenomenon about resemblance between our new binary signal set $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$) and quaternary signal set $\mathcal{S}(m)$ in [15], an awarded work by Kumar, Helleseth, Calderbank, and Hammons. Jr, in 1996. From $\mathcal{S}(m)$ in [15], if we replace the trace function from Galois ring $GR(4,n)$ to Z_4 by the trace function from $\mathbb{F}_{2^n}$ to Z_2, and replace the scalar factor 2 of the sum of those monomial trace terms by a scalar factor 1, and add the sum of the remaining quadratic monomial trace terms with coefficient 1, then $\mathcal{S}(m)$ becomes $\mathcal{S}_o(\rho)$ (or $\mathcal{S}_e(\rho)$) in our construction where $m=\rho$.

References

[1] S. Boztas and P. V. Kumar, Binary sequences with Gold-like correlation but larger linear span, *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 532-537, Mar. 1994.

[2] P. Udaya, Polyphase and frequency hopping sequences obtained from finite rings, Ph.D dissertation, Dept. Elec. Eng., Indian Inst. Technol., Kanpur, 1992.

[3] M. K. Simon, J. Omura, R. Scholtz, and K. Levitt, *Spread Spectrum Communications*, vols. I-III, Computer Science Press, Rockville, 1985.

[4] L. R. Welch, Lower bounds on the maximum cross correlation of the signals, *IEEE Trans. Inform. Theory*, IT-20, pp. 397-399, May 1974.

[5] V. M. Sidelnikov, On the mutual correlation of sequences, *Soviet Math. Dokl,*, vo.12, pp. 197-201, 1971.

[6] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. Inform. Theory*, vol. 14, pp. 154-156, Jan. 1968.

[7] T. Kasami, Weight enumerators for several classes of subcodes of the 2nd-order Reed-Muller codes, *Information and Control*, vol. 18, pp. 369-394, 1971.

[8] S. H. Kim and J. S. No, New families of binary sequences with low correlation, *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3059-3065, Nov. 2003.

[9] A. Chang, P. Gaal, S. W. Golomb, G. Gong, T. Helleseth, and P. V. Kumar, On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code, *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 680-687, Mar. 2000.

[10] J. S. No, S .W. Golomb, G. Gong, H. K. Lee, and P. Gaal, Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation, *IEEE Trans. Inform. Theory*, vol.44, no. 2, pp. 814-817, Mar. 1998.

[11] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

[12] S. W. Golomb and G. Gong, *Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar.* Draft, 2004.

[13] T. Helleseth and P. V. Kumar, *Sequences with Low Correlation*, a chapter in *Handbook of Coding Theory*, edited by V. Pless and C. Huffman, Elsevier Science Publishers, 1998.

[14] O. Moreno and P. V. Kumar, Minimum distance bounds for cyclic codes and Deligne's theorem, *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 1524-1534, Sept. 1993.

[15] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons. Jr., Large families of quaternary sequences with low correlation, *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 579-592, Mar. 1996.